UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/566,510	01/30/2006	Antonius Adriaan Maria Staring	NL030963	7328

24737 7590 12/30/2008
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
12/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/566,510	Applicant(s) STARING ET AL.	
	Examiner Christian LaForgia	Art Unit 2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 September 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 20 October 2008 has been entered.

2. Claims 1-13 have been presented for examination.

Response to Arguments

3. Applicant's amendments, filed 20 October 2008, have been fully considered and are persuasive to overcome the objection to the specification.

4. Applicant's arguments with respect to claims 1-13 have been considered but are moot in view of the new grounds of rejection set forth below.

Claim Rejections - 35 USC § 103

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 1-3 and 6-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2003/0091186 to Fontijn et al., hereinafter Fontijn, in view of U.S. Patent Application Publication No. 2002/0141577 A1 to Ripley et al., hereinafter Ripley.

7. As per claim 1, Fontijn teaches a record carrier (Figures 1, 4, and 5 [block 4]) for storing user data in sectors (paragraph 0003) and management information associated with said sectors

(paragraph 0022, i.e. initialization vector stored in each header or sub-header of each block/sector).

8. Fontijn does not teach wherein said management information comprises an encryption indication information comprising a single bit associated with each of said sectors, each bit indicating to a read-out device whether the user data stored in the associated sector are to be encrypted by a read-out device before being transmitted over a communication bus.

9. Ripley teaches reading a media key block (Figure 3 [block 300]) and computing a media key (Figure 3 [block 310]), which in turn is used to calculate a bus key (figure 3 [block 330]), and the bus key is used to encrypt data transferred from the media or storage reader to the host device or media player (Figure 3 [block 340], 5 [block 540]). Ripley also discusses the content scramble system, hereinafter CSS, which incorporates the Advanced Access Content System, hereinafter AACS. The AACS Specification discloses the use of a single bit called the bus encryption bit to indicate that data is to be encrypted in Sections 4.1 and 4.2. MPEP § 2131.01 discloses that the use of multiple references to show that a characteristic not disclosed in the reference is inherent. The use of a reference that does not precede the filing date is proper when the reference is cited to show a fact that was present in the invention. MPEP § 2124.

10. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the management information comprise an encryption indication information comprising a single bit associated with each of said sectors, each bit indicating to a read-out device whether the user data stored in the associated sector are to be encrypted by a read-out device before being transmitted over a communication bus, since Ripley states at paragraph 0027 that the use of bus encryption dramatically improves the protection for DVD-video content by

"wrapping" a robust protection scheme around the CSS scheme.

11. Regarding claim 2, Fontijn teaches wherein said management information is stored in a sector header or in an additional sub-code channel (paragraph 0022, i.e. initialization vector stored in each header or sub-header of each block/sector).

12. Regarding claim 3, Fontijn teaches wherein said management information further comprises an encryption amount information indicating which part or parts of the user data stored in the associated sector are to be encrypted (paragraphs 0022, 0024, i.e. initialization vector can be used to contain encryption control information).

13. Regarding claim 6, Fontijn teaches wherein said management information further comprises a decryption indication information indicating that the user data stored in the associated sector are to be decrypted by the read-out device before being encrypted again for transmission over said communication bus (paragraph 0048, i.e. data is decrypted and than re-encrypted).

14. With regards to claim 7, Fontijn teaches wherein a decryption key for decryption of the user data is dependent on at least the encryption indication flag (paragraphs 0039, 0040).

15. As per claims 8, 9, and 13, Fontijn teaches a read-out device, method, and computer program product for reading data from a record carrier (Figures 1, 4, and 5 [block 4]) storing

user data in sectors (paragraph 0003) and management information associated with said sectors (paragraph 0022, i.e. initialization vector stored in each header or sub-header of each block/sector) comprising:

a reading unit for reading said user data and said management information from said record carrier (Figures 1 and 4 [block 5], paragraphs 0036, 0037),

a data interpreter for interpreting said management information (paragraphs 0039, 0040, i.e. determining if the data is encrypted or not, determining a decryption key corresponds to the encryption key),

an encryption unit for encrypting user data of sectors for which the associated encryption indication flag indicates that said user data are to be encrypted (Figure 4 [block 10], paragraphs 0022, 0048), and

an output unit for outputting said user data (Figure 4 [block 26], paragraph 0048).

16. Fontijn does not teach wherein said management information comprises an encryption indication information comprising a single bit associated with each of said sectors, each bit indicating whether the user data stored in the associated sector are to be encrypted by a read-out device before being transmitted over a communication bus.

17. Ripley teaches reading a media key block (Figure 3 [block 300]) and computing a media key (Figure 3 [block 310]), which in turn is used to calculate a bus key (figure 3 [block 330]), and the bus key is used to encrypt data transferred from the media or storage reader to the host device or media player (Figure 3 [block 340], 5 [block 540]). Ripley also discusses the content scramble system, hereinafter CSS, which incorporates the Advanced Access Content System, hereinafter AACS. The AACS Specification discloses the use of a single bit called the bus

encryption bit to indicate that data is to be encrypted in Sections 4.1 and 4.2. MPEP § 2131.01 discloses that the use of multiple references to show that a characteristic not disclosed in the reference is inherent. The use of a reference that does not precede the filing date is proper when the reference is cited to show a fact that was present in the invention. MPEP § 2124.

18. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the management information comprise an encryption indication information comprising a single bit associated with each of said sectors, each bit indicating to a read-out device whether the user data stored in the associated sector are to be encrypted by a read-out device before being transmitted over a communication bus, since Ripley states at paragraph 0027 that the use of bus encryption dramatically improves the protection for DVD-video content by "wrapping" a robust protection scheme around the CSS scheme.

19. As per claims 10 and 11, Fontijn teaches a recording device and method for recording data on a record carrier comprising:

an input unit for receiving user data and a command to record said user data in sectors on a record carrier from a communication bus (Figure 5 [block 34], paragraphs 0014, 0051),

a command interpreter for interpreting said command so as to identify a decryption indication information included therein indicating which parts of the received user data are encrypted and are to be decrypted before recording on said record carrier (Figure 5 [block 34], paragraphs 0014, 0051), a decryption unit for decrypting the parts of said user data for which the associated decryption indication information indicates that they are encrypted and are to be decrypted before recording on said record carrier (Figures 1 and 4 [block 8], paragraphs 0040, 0048), and

a write unit for recording said user data in sectors on said record carrier and a management information associated with said sectors (Figure 5 [block 34], paragraphs 0014, 0051).

20. Fontijn does not teach encryption indication information comprising a single bit associated with each of said sectors, each bit indicating whether the user data stored in the associated sector are to be encrypted by a read-out device before being transmitted over a communication bus.

21. Ripley teaches reading a media key block (Figure 3 [block 300]) and computing a media key (Figure 3 [block 310]), which in turn is used to calculate a bus key (figure 3 [block 330]), and the bus key is used to encrypt data transferred from the media or storage reader to the host device or media player (Figure 3 [block 340], 5 [block 540]). Ripley also discusses the content scramble system, hereinafter CSS, which incorporates the Advanced Access Content System, hereinafter AACS. The AACS Specification discloses the use of a single bit called the bus encryption bit to indicate that data is to be encrypted in Sections 4.1 and 4.2. MPEP § 2131.01 discloses that the use of multiple references to show that a characteristic not disclosed in the reference is inherent. The use of a reference that does not precede the filing date is proper when the reference is cited to show a fact that was present in the invention. MPEP § 2124.

22. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the management information comprise an encryption indication information

comprising a single bit associated with each of said sectors, each bit indicating to a read-out device whether the user data stored in the associated sector are to be encrypted by a read-out device before being transmitted over a communication bus, since Ripley states at paragraph 0027 that the use of bus encryption dramatically improves the protection for DVD-video content by "wrapping" a robust protection scheme around the CSS scheme.

23. Regarding claim 12, Fontijn teaches an encryption indication flag and that a decryption key for decryption of the user data is dependent on said encryption indication flag (paragraphs 0039, 0040).

24. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fontijn in view of Ripley as applied above, and in further view of U.S. Patent No. 6,378,072 to Collins et al., hereinafter Collins.

25. Regarding claim 4, Fontijn does not teach an encryption algorithm information indicating which encryption algorithm is to be used for encryption.

26. Collins discloses using a plurality of encryption algorithms to secure a communications bus (column 6, lines 5-27).

27. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include an encryption algorithm information indicating which encryption algorithm is to be used for encryption, since it would have provided a multitude of methods to secure the communication bus against unwanted access during transmission (Fontijn, paragraph 0018).

28. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fontijn in view of Ripley as applied above, and in further view of U.S. Patent Application Publication No. 2003/0159037 to Taki et al., hereinafter Taki.

29. Regarding claim 5, Fontijn does not teach a key-hierarchy information indicating which key-hierarchy is to be used for determination of an encryption key to be used for encryption.

30. Taki teaches a key-hierarchy information indicating which key-hierarchy is to be used for determination of a content key (Figures 4, 8, 23, paragraph 0001).

31. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a key-hierarchy information indicating which key-hierarchy is to be used for determination of an encryption key to be used for encryption, since Taki states at paragraph 0001 that a key hierarchy is used for digital rights management and to ensure authorized use of the content.

Conclusion

32. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

33. The following patents are cited to further show the state of the art with respect to content scrambling systems, such as:

United States Patent Application Publication No. 2002/0141578 A1 to Ripley et al., which is cited to show the published application of the patent that was previously used to reject the claims of the instant application.

United States Patent Application Publication No. 2002/0015494 A1 to Nagai et al., which is cited to show protecting content on a medium.

34. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

35. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

36. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

clf